UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
08/999,766	07/23/1997	SCOTT A. MOSKOWITZ	80410.0009	4344

7590 01/31/2008

Scott A. Moskowitz
Wistaria Trading, Inc.
16711 Collins Avenue, #2505
Sunny Isles Beach, FL 33160

EXAMINER	
CALLAHAN, PAUL E	
ART UNIT	PAPER NUMBER
2137	
MAIL DATE	DELIVERY MODE
01/31/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

RECORD OF ORAL HEARING

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte SCOTT A. MOSKOWITZ and MARC COOPERMAN

Appeal 2007-2273
Application 08/999,766
Technology Center 2100

Oral Hearing Held: December 19, 2007

Before LANCE LEONARD BARRY, HOWARD B. BLANKENSHIP, and JAY P. LUCAS, *Administrative Patent Judges*.

ON BEHALF OF THE APPELLANT:

SCOTT WOFSY, ESQUIRE
Edwards, Angell, Palmer & Dodge
301 Tresser Boulevard
Stamford, Connecticut 06901

The above-entitled matter came on for hearing on Wednesday, December 19, 2007, commencing at 10:24 a.m., at The U.S. Patent and Trademark Office, 600 Dulany Street, Alexandria, Virginia, before Carol A. Lowe, RPR, CCR No. 0313084, Notary Public.

P R O C E E D I N G S

JUDGE LUCAS: Mr. Wofsy.

MR. WOFSY: Yes, sir.

JUDGE LUCAS: Welcome.

MR. WOFSY: Thank you very much. If you would just give me one moment to get set here. If I may make a few introductions this morning, please.

JUDGE BARRY: Please.

MR. WOFSY: I am Scott Wofsy, Registration Number 35413, with the law firm of Edwards, Angell, Palmer & Dodge out of the Stamford office in Connecticut.

I am joined today by the inventor, Mr. Scott Moskowitz, and one of the investors in the subject matter of the invention, Mr. Mark Stein.

JUDGE BARRY: Welcome.

JUDGE LUCAS: Welcome, everybody. Happy holidays to all of you.

MR. WOFSY: Thank you. Same to you. May I approach --

JUDGE BARRY: Please.

MR. WOFSY: -- for one moment?

This is -- actually, I'm going to hold onto one of them. This is a physical embodiment of the invention. And maybe that's where I'll begin.

The subject matter of the application that has been pending for quite some time now is a method of watermarking digital content so as to identify copies of the original content that was originally licensed to a specific party.

Now, I've presented you with a copy of a physical embodiment of an audio disk. Please don't ask me any of the songs that are on this disk, because I don't think I could tell you that.

But I can tell you what is on this. And that is a digital watermark. And you can see the disclaimer language that is imprinted. It says, this CD has been individually watermarked with a unique identification number embedded in the music. This number is traceable directly to the authorized recipient, you, which allows us to identify the source of any unauthorized copies or reproductions.

And you can see on the physical CD there it belongs to Miss Ashley White and has a number 142 associated with it.

So this disk right here has on it the digital watermark that has been placed or embedded into the audio signal using the method of the subject invention.

Now, the subject invention relates to steganography and cryptography. Cryptography is a technique of scrambling a message so that only a recipient of the message can read it.

Steganography, on the other hand, is a technique of obscuring or hiding a message in plain sight so that only the intended parties to a message even know that a message has been sent.

JUDGE BARRY: Not to be confused with paleontology in this case.

MR. WOFSY: Well, you know --

MR. MOSKOWITZ: Or stenography.

MR. WOFSY: Or stenography, right, which is also going on in this room.

But, in any event, we are talking about something in this case called a stega-cipher. It's a thing. And it is the basis for the 112 rejection that is presently pending in the file history.

The 112, paragraph 1 rejection is based on the definition of the term "stega-cipher" which was incorporated into the claims late in prosecution; but, nevertheless, it was considered by the examiner.

And the rejection specifically with respect to stega-cipher which is a noun, not a verb as proposed by the examiner in three separate definitions in his answer -- the noun is a thing that is basically an algorithm.

It's a two-part algorithm. The first part of the algorithm, the stega part, is a -- basically is a function that determines a set of potential locations in a carrier signal where you can place the message or parts of the message.

And then the cipher part -- stega-cipher. The cipher part is actually the encoding part. It encodes, it hides, it obfuscates the message within the carrier signal.

So we have a thing, a two-part function. And it is clearly described in the specification so that a person of ordinary skill in the art reading the specification would know what the term means.

And this was a -- it was found in the original specification, in the original claims, as a matter of fact, in the original written claims that were filed early on. And we mention that in the appeal brief.

JUDGE BARRY: This is a written description rejection.

MR. WOFSY: Yes.

JUDGE LUCAS: Right.

JUDGE BARRY: So if it's in the original claims which are part of the original spec, where is the basis for a written description rejection?

MR. WOFSY: I agree with you. There is no basis.

JUDGE LUCAS: That's not what he has to argue.

MR. WOFSY: The actual argument -- excuse me. The rejection is that there is no support for the use of the message itself that you are hiding in the formation of a key or a mask set.

Now -- so the mask set is a critical part of what a stega-cipher is. So a stega-cipher is something that uses the -- it creates a mask set that involves a random seed or a pseudorandom seed that creates the mask set and uses the message itself.

And the support for that can actually be found at pages 39 through 41 of the original specification which was one of the original claims. It was claim 3 of the specification.

JUDGE LUCAS: Well, let's look at page 7 --

MR. WOFSY: Page 7.

JUDGE LUCAS: -- of the specification, if you wouldn't mind, Mr. Wofsy.

MR. WOFSY: Certainly.

JUDGE LUCAS: Okay.

MR. WOFSY: I'm with you. Stega-cipher. Yes.

JUDGE LUCAS: Okay. At the bottom of page 7 we have a -- what looks to me to be a definition of stega-cipher. (Reading from the specification, “The stega-cipher is so named because it uses the

steganographic technique of hiding messages in multimedia content, and so forth." Would you read that section?

MR. WOFSY: The section you're referring to, I believe, is between lines 15 and 20.

JUDGE LUCAS: It starts there.

MR. WOFSY: "The stega-cipher is so named because it uses the steganographic technique of hiding a message in multimedia content in combination with multiple keys, a concept originating in cryptography." Yes. So --

JUDGE LUCAS: Keep going. I think that this is important, because this is the broadest definition of stega-cipher that you have.

MR. WOFSY: Okay. "And instead of using keys to encrypt the content, the stega-cipher uses these keys to locate the hidden message within the content." That's actually the decode aspect of it.

So the stega-cipher is using -- is encoding the message, hiding or obfuscating the message within the carrier signal. And you use the same key or the same mask set to decode.

Now, the mask set is something that is generated using the original message. And the part of the original message that is used is something called a message delimiter. And also he uses the number of bits or a 32-bit aspect of the size of the message that you're going to be encoding.

So these aspects of the message are part of what is used to generate the mask set or the keys.

JUDGE LUCAS: Okay. In carefully reviewing the spec would you say that this is the definition that we should be relying on to establish that the inventor sufficiently grasped the nature of the invention?

MR. WOFSY: It is a example of where the term can be defined in the specification. Is that the --

JUDGE LUCAS: Is there a better definition that you want to depend upon or is this the --

MR. WOFSY: Well, it is -- I believe it's the broadest definition --

JUDGE LUCAS: Right.

MR. WOFSY: -- of what a stega-cipher is; but the rejection was based upon the fact that the examiner did not believe that the message itself was used to generate the mask set or the key.

And that -- therein lies the problem with the rejection, because it clearly -- the specification clearly states that the message itself is used or parts of the message is used to create the key. So the 112 rejection must fall.

JUDGE LUCAS: But the 112 rejection can fall if there is a sufficient definition of stega-cipher --

MR. WOFSY: The definition that you --

JUDGE LUCAS: -- to just prove that the inventor grasped the true metes and bounds of his invention at the time.

MR. WOFSY: He did. The inventor was in possession of the broadest statement of the term "stega-cipher" at the time of filing.

JUDGE LUCAS: Right.

MR. WOFSY: There's no doubt about that. And I believe you found in the specification or highlighted what could be the broadest reference to stega-cipher, the term, the noun stega-cipher.

JUDGE LUCAS: When we look at the claim 25 --

MR. WOFSY: Yes.

JUDGE LUCAS: -- which is your -- the broadest claim for at least the encoding side of this, all right, was it -- claim 29 is the --

MR. WOFSY: 29 is decode. 25 is the encode.

JUDGE LUCAS: -- is the decode. And 25 is the code.

MR. WOFSY: Yeah.

JUDGE LUCAS: 25 has not much more than saying give a carrier signal. The carrier signal, by the way, are you now saying that it could only be audio?

MR. WOFSY: No. This could be audio, visual.

JUDGE LUCAS: Or visual

MR. WOFSY: It's any kind of signal.

JUDGE LUCAS: Right. And then using a stega-cipher to steganographically -- it took a while to be able to pronounce that --

MR. WOFSY: You're not the only one that has trouble with that word.

JUDGE LUCAS: -- encode independent information -- that's the message -- including a digital watermark into the carrier signal in the claim.

MR. WOFSY: Right.

JUDGE LUCAS: So really in order to properly find the metes and bounds of this claim I have to find the reasonable definition. I found one on page 7. Is that one that you're willing to rely on?

MR. WOFSY: It is -- I am willing to rely upon a broad definition of the term "stega-cipher" that you have highlighted on page 7. That is one of the definitions that -- or one aspect of the definition as proposed during briefing.

JUDGE LUCAS: Yes. I'm not trying to trap you.

MR. WOFSY: Okay. Not a problem. Not looking to be trapped. And I understand you're trying to help out. What we were concerned with was the examiner's additional definitions that were proposed in his answer that hadn't been discussed during prosecution.

JUDGE LUCAS: You and the examiner tended to get off into certain enthusiastic arguments against each other which I deplore on both sides, I must say. But -- okay. If we settle that you're willing to live with this, then we have a basis, I think, for resolution of the 112.

MR. WOFSY: Okay. Fair.

JUDGE LUCAS: Okay. I'm sorry to interrupt, but I think that was an important preliminary point.

MR. WOFSY: Yes. Once the 112 issue, I think, is resolved and we understand that a stega-cipher is a unique being, a unique thing, then its comparison in the claims or comparing the claims to the prior art I think helps us in overcoming the anticipatory references and the obviousness rejections.

If we were to compare now what a claim that involves the use of a stega-cipher is compared to, for example, what Bender teaches --

JUDGE LUCAS: Okay.

MR. WOFSY: -- Bender is a reference -- excuse me. Bender is the technique for hiding data. It's the publication. Bender is essentially a spread-spectrum technique.

What Bender does is -- rather than hiding or obfuscating a message in discrete, random locations within the carrier signal Bender chooses and teaches to spread the signal over as much of the available frequency as possible.

This is very distinct from what we're doing. There is -- there's no stega-cipher that is used in terms of encoding or hiding the message. You simply are modulating and demodulating. It's totally different.

JUDGE LUCAS: Well, are you really trying to say that Bender has absolutely no reference to steganographic techniques?

MR. WOFSY: It is not using a stega-cipher. It is not steganographic technique. It is simply a modulation of a signal to create noise that is overlaid upon the carrier. It's -- and as many -- across the entire frequency of the carrier signal.

So you are not selecting random points that are available or locations to place your message in plain sight.

JUDGE LUCAS: Okay. Bender seems to have two aspects to it, doesn't he, the visual and the audio?

MR. WOFSY: Correct.

JUDGE LUCAS: And does he not try to hide in plain sight a message -- at least in the visual side?

MR. WOFSY: Even if it's in a visual signal, you're still using -- you're still overlaying the -- you're not encrypting, first of all. You're taking a modulated signal and -- or a modulated message. And you're overlaying it upon or adding it to or multiplying it to the carrier.

There is no -- there's no key that is used to encode whereas in a stega-cipher using our mask set that is generated as a key.

JUDGE LUCAS: What about that reference to prior work on page 2 of Bender where it mentions that the key can be encrypted?

MR. WOFSY: You're referring to 1.2, prior work by Adelson?

JUDGE LUCAS: No, actually 1.2, prior work -- yes, but there's a sentence in there having to do with his prior work where he mentions that --

MR. WOFSY: You're talking about the encryption of data?

JUDGE LUCAS: Yes.

MR. WOFSY: Well, the encryption of data is -- that's encrypting the message. We're not talking about encrypting the message. We're talking about encoding the message.

JUDGE LUCAS: What about the chaos thing? Bender modifies --

MR. WOFSY: Bender modifies by using chaos as a means to encrypt --

JUDGE LUCAS: . . . the embedded data.

MR. WOFSY: Well, you're -- that's encrypting the message.

JUDGE LUCAS: Right.

MR. WOFSY: Encryption of a message, that could be something that we do; but that's not the same as embedding using a stega-cipher function.

The encryption of a message, that is known. I mean, that's -- you can encrypt a message -- in fact, we teach encryption of a message as a secondary way of guaranteeing our signal quality.

JUDGE BARRY: It's not in your claim, but isn't that correct? You encrypt the message first. And then you embed the encryption message.

MR. WOFSY: It's optional. It's optional. You can. It's an added safety feature.

JUDGE BARRY: Sure.

MR. WOFSY: So you can encrypt the message, but after you've encrypted it now you're using the stega-cipher function to encode it.

JUDGE BARRY: Okay.

MR. WOFSY: It's an overlaying of technology here.

JUDGE BARRY: Right.

MR. WOFSY: So the encoding is where you're placing it in the discrete locations in plain view. Okay. And that is the stega part of it.

So, again, there is nothing in Bender that teaches or discloses in any way, shape or form a stega-cipher function.

JUDGE LUCAS: Okay. That's your position. And I appreciate that being your position. Continue.

MR. WOFSY: In terms of Powell which is the other 102 reference that we are presented with, I can speak of Powell with respect to the EP as well as the U.S. reference that was applied. The EP reference is the 0581317

reference. And Powell, 5930377. Those were both references that were utilized by the examiner.

Powell is a way of -- well, first of all, there's no cipher that is used here. We're not talking about any key that is used to encrypt or encode.

What they're doing here is they are selecting what they -- pixels in a video image to place a signature. And these pixels are selected. They're called -- they call them extrema. They look for extreme pixels of -- extrema. E-X-T-R-E-M-A.

They are pixels that are located because they have an intense brightness or a high intensity. They differentiate between some other type of pixel.

And they select them. And they change them by putting -- selecting that location to put the signature, the digital signature in this case, not to be confused with real digital signatures; but it's a digitized signature. And they overlay it on the message, on the -- on the image.

You need the original image to extract the signature. You have to do a comparison. That's not cryptography. That -- at best it's -- you're placing it in plain view by altering the image.

So this is not a situation where you use a random seed to generate a mask set to then encode a message into a carrier signal. It's just not the case. It's not the same thing.

So Bender is -- excuse me. Powell is distinct from the claimed invention.

JUDGE LUCAS: The difficulty I have, Mr. Wofsy, is that you have to -- in looking at 25, you see how minimalist the claim is. It mentions using

a stega-cipher. Okay. The claim itself does not say what a stega-cipher is. We go back to the specification.

And the question is how much of the specification is defining a term in the claim versus how much is reading the entire specification into the claim.

There's a judgment call that has to be made. This is not a classic claim in which you have elements A, B, C, all of which are well known; but rather it's a claim in which you have elements A and B. And element B has to be defined by the specification. And yet we don't want to read all 50 pages of the specification into the --

MR. WOFSY: There's no need to read all 50 pages of the specification into the claim. There are very succinct aspects of the specification that explain that a stega-cipher uses a mask set; that that is throughout the specification.

The key and the mask set are one in the same. The mask set is defined as a random generated key that is created by the frequency key. Then there's a random generated convolution set. And then there's the message delimiter set.

These masks -- this mask set is the essence of what a stega-cipher is. It's just like a mask work in a copyright. You overlay the mask work over the original carrier signal. And you can then decode by lifting the mask set.

That is the quintessential aspect of what a stega-cipher is. It is the use of -- it is a function that uses a mask set or a mask set that's generated. It's keys. That's the cipher aspect of it.

Now, as to the 103 references, the 103 references can be grouped. I can group them as cryptographic references that use encryption technology. [Buzzer sounds.] Are we done?

JUDGE LUCAS: Well, finish the sentence, please.

MR. WOFSY: Okay. Encryption technology. And then I can -- the other group would be spread-spectrum references that simply spread a modulated wave or noise over the signal as a way of encrypting the message into the carrier.

JUDGE LUCAS: Okay.

MR. WOFSY: Thank you, gentlemen.

JUDGE LUCAS: Thank you for coming in.

JUDGE BARRY: Thank you all.

MR. MOSKOWITZ: Can I have one comment? Do you mind? Just one. It's one sentence.

JUDGE LUCAS: Okay. Is this off the record?

MR. MOSKOWITZ: That's fine, too.

JUDGE BARRY: No, actually, if it's --

MR. MOSKOWITZ: It will help clear things up. I mean, I've been involved in this for a long time.

JUDGE BARRY: Well, why don't we do it on the record.

JUDGE LUCAS: Yes, put it on the record.

JUDGE BARRY: Put it on the record, please.

MR. MOSKOWITZ: The way that I would characterize Bender, it's not encryption. It's spread-spectrum. There is a pseudorandom sequence

which he parenthetically treats the term "key," because it's not a key. It's not an index of functions. It's not a mask set.

It's a single input which spreads and a single input that comes out by de-spreading. So possession of what would be akin to a stega-cipher for Bender reveals everything. There is no security that accrues.

The steganographic cipher, although it is a short claim, I characterize it as a pioneering patent. It's an answer to a solution for copyright problems.

And you require two inputs. You have one input which is the message and one input which is the key. And because you have two inputs you end up with a completely different mind-set and a completely different way of approaching the problem of copyright protection.

But each of the cited references can only be characterized as either having a single input, which necessarily impacts the signal itself and, thus, on decode either has to rely on original or becomes or returns itself to the same state.

So steganographic cipher is two inputs. A traditional cipher is a single input.

JUDGE LUCAS: Thank you.

MR. WOFSY: Thank you.

MR. MOSKOWITZ: Thank you for the time.

(Whereupon, the proceedings at 10:45 a.m. were concluded.)